

ELECTRONIC WATERMARKING METHOD AND SYSTEM

FIELD OF THE INVENTION

The present invention relates to an electronic watermarking technique for digital data, and in particular to a practical and robust electronic watermarking technique.

BACKGROUND

Conventionally, electronic watermarking techniques fall into a category wherein a theoretical electronic watermarking method is applied unchanged for a variety of products, and no truly practical technique has been provided that can prevent the analyzation of an embedding algorithm. As an example, an electronic watermarking technique for digital data, an embedding and detection method used for a frequency domain, is disclosed in USP 5,687,236. According to this conventional electronic watermarking technique, embedded additive information is detected so that it can be synchronized with information (embedding start information) indicating the start of embedding. With this method, however, in addition to the additive information that originally is embedded, a synchronization signal is provided that must be used when detecting the embedded additive information. This signal must, therefore, be detected first, and accordingly, additional time is required for this purpose. Further,

099443-02204

1 when a third party, with larcenous intent, detects a
2 synchronization signal, that party can easily analyze and
3 extract all the embedded information. Therefore, it is
4 generally acknowledged that a need exists for a practical
5 and robust electronic watermarking technique.

6 **SUMMARY OF THE INVENTION**

7 To resolve the problems inherent to conventional
8 electronic watermarking techniques, it is one object of
9 the present invention to provide a practical and robust
10 electronic watermarking method and system.

11 It is another object of the present invention to provide
12 an electronic watermarking method and system for which,
13 when they are employed for the detection of embedded
14 additive information, a synchronization signal is not
15 required.

16 It is an additional object of the present invention to
17 provide an electronic watermarking method and system for
18 reducing the time required for detecting embedded
19 additive information.

20 It is a further object of the present invention to
21 provide an electronic watermarking method and system for
22 protecting an embedding algorithm and preventing it from
23 being easily analyzed.

1 BRIEF DESCRIPTION OF THE DRAWINGS

2 These and other objects, features, and advantages of the
3 present invention will become apparent upon further
4 consideration of the following detailed description of
5 the invention when read in conjunction with the following
6 drawing figures:

7 Fig. 1 is an example of a flowchart for a practical and
8 robust electronic watermark embedding method according to
9 the invention.

10 Fig. 2 is an example of a flowchart for a practical and
11 robust electronic watermark detection method according to
12 the invention.

13 Fig. 3 is an example of a graph for explaining a time
14 axis, a frequency axis and bit embedding.

15 Fig. 4 is a diagram for explaining frame overlapping.

16 Fig. 5 is a diagram for explaining an amplitude change.

17 Fig. 6 is a diagram for explaining windowing and frame
18 overlapping.

19 Fig. 7 is a diagram for explaining an example wherein
20 there is no frame shift.

21 Fig. 8 is a diagram for explaining a one frame shift.

- 1 Fig. 9 is a diagram for explaining cycle synchronization.
- 2 Fig. 10 is a diagram showing an example wherein a wide
- 3 frequency band is allocated while half of the additive
- 4 information is regarded as more important.
- 5 Fig. 11 is a diagram for explaining diagonal embedding.
- 6 Fig. 12 is a diagram for explaining discrimination and
- 7 equalization of reliability.
- 8 Fig. 13 is a diagram for explaining diagonal embedding
- 9 that can increase the processing speed.
- 10 Fig. 14 is a diagram for explaining the pre-process and
- 11 the post-process for the embedding process.
- 12 Fig. 15 is a diagram for explaining a method for
- 13 performing re-sampling and calculating an embedding
- 14 signal.
- 15 Fig. 16 is an example of a diagram for explaining another
- 16 method for performing re-sampling and calculating an
- 17 embedding signal.
- 18 Fig. 17 is a diagram for explaining an embedding start
- 19 unit.
- 20 Fig. 18 is a diagram for explaining a virtual embedding
- 21 start position.

1 Fig. 19 is a diagram showing a bit information embedding
2 position that is changed as time elapses.

3 Fig. 20 is a diagram showing an example of the insertion
4 of a non-information embedding position.

5 Fig. 21 is a diagram showing an example wherein
6 information is embedded for which the bit is inverted at
7 cycle 2T.

8 Fig. 22 is a diagram showing an example use of
9 information other than bit information.

10 **DETAILED DESCRIPTION OF THE INVENTION:**

11 The present invention provides methods, systems and
12 apparatus to achieve these and other objects. Thus,
13 according to a first aspect of the invention, an
14 electronic watermarking system, for embedding additive
15 information in digital data, for which one frame is
16 defined as including N samples extracted from digital
17 data and a current frame is defined as a frame that is
18 overlapped by M samples ($0 < M \leq N/2$) of a preceding frame,
19 comprises: a frequency domain transformation unit, for
20 multiplying a frame extracted from digital data by a
21 window function, and for using the results to perform a
22 Fourier transform and thus obtain a frequency component
23 for the digital data; a frequency domain embedding unit,
24 for employing bit information for additive information,
25 and a frequency band for the frequency component to

1 change the amplitude of the frequency component in the
 2 digital data obtained by the frequency domain
 3 transformation unit; a time domain transformation unit,
 4 for performing an inverse Fourier transform to return, to
 5 a time domain signal, the frequency component whose
 6 amplitude has been changed by the frequency domain
 7 embedding unit; and an additive information embedding
 8 frame generator, for multiplying, by a window function,
 9 the time domain signal obtained by the time domain
 10 transformation unit, and for superimposing overlapped
 11 frames to generate a frame wherein the additive
 12 information is embedded.

13 Advantageously, to change the amplitude of the frequency
 14 component of the digital data, the frequency domain
 15 embedding unit employs bit information for additive
 16 information and the values of a mask, determined in
 17 advance in accordance with a frequency band, with which
 18 the frequency component is to be increased or decreased.
 19 advantageously, the values of the mask corresponding to
 20 all the frequencies included in one frequency band are
 21 equalized.

22 Advantageously, as the frequency increases, the width of
 23 the frequency band is extended.

24 According to a second aspect of the invention, an
 25 electronic watermark detection system, for detecting
 26 additive information embedded in digital data, comprises:
 27 a frequency domain transformation unit, for multiplying a

1 frame extracted from digital data by a window function,
 2 and for performing a Fourier transform to obtain a
 3 frequency component from the digital data; an amplitude
 4 storing unit, for obtaining amplitudes for the frequency
 5 components acquired by the frequency domain
 6 transformation unit, and for storing a number of the
 7 amplitudes that equals a predetermined frame count; a
 8 cycle synchronization unit, for employing an amplitude
 9 value stored by the amplitude storing unit to designate a
 10 bit detection start frame; and a bit detector, for
 11 detecting bit information from embedded additive
 12 information beginning at the bit detection start frame
 13 obtained by the cycle synchronization unit.

14 Advantageously, the frequency domain transformation unit
 15 uses the shorter length of the frame than the length when
 16 the additive information is embedded.

17 Advantageously, in order to designate the bit detection
 18 start frame by referring to the amplitude values, the
 19 cycle synchronization unit employs calculation results
 20 obtained by using the values of a mask that defines, in
 21 advance, a frequency component increase or decrease.

22 According to a third aspect of the invention, an
 23 electronic watermarking method, for embedding additive
 24 information in digital data, whereby one frame is defined
 25 as including N samples extracted from digital data, and a
 26 current frame is defined as a frame that is overlapped by
 27 M samples ($0 < M \leq N/2$) of a preceding frame, comprises the

1 steps of: extracting one frame as a current frame from
 2 digital data; multiplying the current frame by a window
 3 function; performing a Fourier transform for the
 4 resultant current frame to obtain a frequency component
 5 for the current frame; changing an amplitude of the
 6 frequency component in accordance with bit information
 7 for additive information; performing an inverse Fourier
 8 transform for the resultant frequency component;
 9 multiplying, by the window function, the frequency
 10 component obtained using the inverse Fourier transform;
 11 and adding an (N-M)-th sample, from the end of a
 12 preceding frame processed in the same manner, to an M-th
 13 sample, from the head of the current frame, and
 14 generating one new frame including N samples.

15 Advantageously, at the step of changing the amplitude of
 16 the frequency component, the amplitude is changed by
 17 employing bit information for additive information and
 18 the values of a mask, determined in advance in accordance
 19 with a frequency band, with which the frequency component
 20 is to be increased or decreased.

21 Advantageously, the values of the mask corresponding to
 22 all the frequencies included in one frequency band are
 23 equalized.

24 Advantageously, as the frequency increases, the width of
 25 the frequency band is extended.

26 According to a fourth aspect of the invention, a method

1 for detecting additive information embedded in digital
 2 data comprises the steps of: extracting one frame
 3 including N samples from digital data; multiplying the
 4 frame by a predetermined window function; performing a
 5 Fourier transform for the resultant frame to obtain a
 6 frequency component of the frame; storing a value for an
 7 amplitude of the frequency component; calculating an
 8 optimal start frame for additive information detection
 9 when the stored amplitude value reaches a predetermined
 10 value; and detecting bit information for the additive
 11 information beginning at the start frame.

12 Advantageously, at the step of extracting one frame, uses
 13 the shorter length of the frame than the length when the
 14 additive information is embedded.

15 Advantageously, at the step of calculating the optimal
 16 start frame, calculation results obtained by using the
 17 values of a mask, which define, in advance, a frequency
 18 component increase or decrease, are employed in order to
 19 designate the bit detection start frame by referring to
 20 the amplitude value.

21 According to a fifth aspect of the invention, an
 22 electronic watermarking method for embedding in digital
 23 data N bits ($N \geq 1$) of additive information comprises the
 24 steps of: reading sample values, from digital data, up to
 25 an R-th sample ($R \geq 1$); reading sample values, from the
 26 digital data, following an (R+1)-th sample; changing the
 27 sample values following the (R+1)-th sample in accordance

1 with bit information for additive information; and adding
2 together the values up to the R-th sample in the digital
3 data and the values following the (R+1)-th sample,
4 changed in accordance with the bit information for the
5 additive information.

6 According to a sixth aspect of the invention, an
7 electronic watermarking method for embedding in digital
8 data N bits ($N \geq 1$) of additive information comprises the
9 steps of: reading a sample value from digital data;
10 starting to change the sample value in accordance with
11 bit information for additive information, excluding a
12 head bit of the additive information; and using the
13 changed sample value to generate new digital data.

14 According to a seventh aspect of the invention, an
15 electronic watermarking method for embedding in digital
16 data N bits ($N \geq 1$) of additive information comprises the
17 steps of: reading a sample value from digital data;
18 changing the sample value in accordance with bit
19 information for additive information; adding noise at
20 random to the changed sample value; and using the changed
21 sample value to generate new digital data.

22 According to an eighth aspect of the invention, an
23 electronic watermarking method for embedding in digital
24 data N bits ($N \geq 1$) of additive information comprises the
25 steps of: reading a sample value from digital data;
26 changing the sample value in accordance with bit
27 information for additive information, and setting at

JP919990241US1

1 random a case wherein a change is not required; and using
2 either the changed sample value or the unchanged sample
3 value to generate new digital data.

4 According to a ninth aspect of the invention, an
5 electronic watermarking method for embedding in digital
6 data N bits ($N \geq 1$) of additive information comprises the
7 steps of: changing digital data by superimposing,
8 inserting, deleting or shifting a specific sample of the
9 digital data; reading a sample value from the digital
10 data; changing the sample value in accordance with bit
11 information for additive information; and using the
12 changed sample value to generate new digital data.

13 According to a tenth aspect of the invention, an
14 electronic watermarking method for embedding in digital
15 data N bits ($N \geq 1$) of additive information comprises the
16 steps of: expanding or compressing digital data along a
17 time axis; reading a sample value from the digital data;
18 changing the sample value in accordance with bit
19 information for additive information; and using the
20 changed sample value to generate new digital data.
21 advantageously, the expansion/compression rate for the
22 digital data does not exceed 1%.

23 According to an eleventh aspect of the invention, an
24 electronic watermarking method for embedding in digital
25 data N bits ($N \geq 1$) of additive information comprises the
26 steps of: reading a sample value from the digital data;
27 changing the sample value in accordance with bit

1 information for additive information; using the changed
2 sample value to generate new digital data; and expanding
3 or compressing the new digital data along a time axis.
4 advantageously, the expansion/compression rate for the
5 new digital data does not exceed 1%.

6 According to a twelfth aspect of the invention, an
7 electronic watermarking method for embedding in digital
8 data N bits ($N \geq 1$) of additive information comprises the
9 steps of: re-sampling digital data at a sampling
10 frequency r' and reading a sample value from the digital
11 data; changing the sample value in accordance with bit
12 information for additive information; and sampling the
13 changed sample value at the original sampling frequency r
14 to generate new digital data.

15 According to a thirteenth aspect of the invention, an
16 electronic watermarking method for embedding in digital
17 data N bits ($N \geq 1$) of additive information comprises the
18 steps of: sampling digital data at a sampling frequency
19 r' and reading a sample value from the digital data;
20 obtaining a change in the sample value in accordance with
21 bit information for additive information; re-sampling the
22 change at a sampling frequency r for the original digital
23 data; and adding the re-sampled change to the original
24 digital data to generate new digital data.

25 According to a fourteenth aspect of the invention, an
26 electronic watermarking method for embedding in digital
27 data N bits ($N \geq 1$) of additive information comprises the

1 information embedding frame generation function, for
 2 multiplying, by a window function, the time domain signal
 3 obtained by the time domain transformation function, and
 4 for superimposing overlapped frames to generate a frame
 5 wherein the additive information is embedded.

6 According to a sixteenth aspect of the invention, a
 7 computer-readable recording medium is provided on which a
 8 program for detecting additive information embedded in
 9 digital data is stored, the program permitting a computer
 10 to execute: a frequency domain transformation function,
 11 for multiplying a frame extracted from digital data by a
 12 window function, and for performing a Fourier transform
 13 to obtain a frequency component from the digital data; an
 14 amplitude storing function, for obtaining amplitudes for
 15 the frequency components acquired by the frequency domain
 16 transformation function, and for storing a number of the
 17 amplitudes that equals a predetermined frame count; a
 18 cycle synchronization function, for employing an
 19 amplitude value stored by the amplitude storing function
 20 to designate a bit detection start frame; and a bit
 21 detection function, for detecting bit information from
 22 embedded additive information beginning at the bit
 23 detection start frame obtained by the cycle
 24 synchronization function.

25 **Example Embodiments**

26 Example embodiments of the present invention will now be
 27 described while referring to Figs. 1 to 22. The

1 definitions of terms used for the embodiment are shown in
 2 Table 1, and the list of symbols is shown in Table 2. In
 3 the embodiments of the invention, an explanation will be
 4 given for an example method and an example system for
 5 employing digital audio data as example digital data for
 6 electronic watermarking. However, the electronic
 7 watermarking method and system can be applied in the same
 8 manner for digital moving picture data (MPEG, etc).

9 <First Embodiment>

10 An explanation will be given for a practical and robust
 11 electronic watermarking method and system according to a
 12 first embodiment for which frame synchronization for
 13 digital audio data is not required.

14 An embedding system comprises the following functions.

15 (1) Frequency domain transformation unit

16 * extraction of samples

17 Extracts N samples from digital audio data.

18 * multiplication of window function

19 Multiplies the extracted digital audio data by a
 20 window function.

21 * FFT

22 Performs a FFT to obtain a frequency component.

23 (2) Frequency domain embedding unit

24 The frequency domain embedding unit changes the
 25 amplitude of the frequency component, obtained by
 26 the frequency domain transformation unit, in
 27 accordance with bit information for additive
 28 information and the frequency band of the frequency

1 component. During this process, the frequency
2 domain embedding unit applies an auditory
3 psychological model for the frequency component, and
4 calculates a permissible range wherein even when the
5 amplitude is changed, such a change is not discerned
6 by human beings. Then, within the permissible
7 range, the frequency domain embedding unit changes
8 the frequency component of the digital audio data.

9 (3) Time domain transformation unit

10 The time domain transformation unit performs an IFFT
11 for the frequency component that has been changed.
12 By using an inverse Fourier transform, the time
13 domain transformation unit returns, to a time domain
14 signal, the frequency component whose amplitude was
15 changed.

16 (4) Additive information embedding frame generator

17 The additive information embedding frame generator
18 multiplies, by a window function, a time domain
19 signal obtained by the time domain transformation
20 unit, and superimposes overlapping (adjacent) frames
21 to generate a frame in which additive information is
22 embedded.

23 A detection system comprises the following functions.

24 (1) Frequency domain transformation unit

25 * extraction of a sample

26 Extracts N samples from input digital audio data.

27 * multiplication of a window function

28 Multiplies extracted digital audio data by a window
29 function.

1 * FFT
2 Performs a FFT to obtain a frequency component.
3 (2) Amplitude storing unit
4 Obtains an amplitude from a frequency component, and
5 stores amplitudes in a number equivalent to a
6 predetermined frame count.
7 (3) Cycle synchronization unit
8 The cycle synchronization unit designates a bit
9 detection start frame based on the amplitude value
10 stored by the amplitude storing unit. Values
11 detected by the frequency domain detector are stored
12 in a number equivalent to a predetermined frame
13 count, and a search of the stored values is
14 performed for the greatest absolute value, which
15 subsequently is output as a frame shift. That is, a
16 frame shift is effected in order to determine which
17 frame should be the first for bit detection.
18 (4) Bit detector
19 The bit detector detects bit information for
20 embedded additive information, beginning at the
21 detection start frame designated by the cycle
22 synchronization unit. Each bit is detected and
23 output, based on the frame shift effected by the
24 cycle synchronization unit.

25 Fig. 1 is an example of a flowchart for a practical and
26 robust electronic watermark embedding method according to
27 the embodiment. First, at step 110 one frame (N samples)
28 is extracted from input digital data. At step 120 the
29 extracted frame is multiplied by a window function, and

1 at step 130 a Fourier transform is performed for the
2 resultant frame. As a result, the frequency component of
3 the frame is obtained. Then, at step 140, the amplitude
4 of the frequency component of the frame transformed into
5 the frequency domain is changed in accordance with the
6 additive information, while the phase of the frequency
7 component is maintained. At this time, whether the
8 amplitude should be increased or reduced is determined by
9 using bit information for the additive information to be
10 embedded in the frame and the sign of a mask
11 corresponding to the frequency band of the frame. A
12 change value determined by an auditory psychological
13 model unit is employed as the amount the amplitude is to
14 be changed. It should be noted that this change value is
15 so calculated that, even when digital data is altered, no
16 change in tone quality is discernible by human beings.
17 At step 150, an inverse Fourier transform is performed
18 for the frequency component in which the information has
19 been embedded (the frequency component whose amplitude is
20 changed) to return the frequency component to a signal in
21 the time domain. At step 160, the obtained signal in the
22 time domain is again multiplied by the window function.
23 Finally, the resultant frame is superimposed on the
24 preceding frame to generate a frame wherein additive
25 information is embedded.

26 Fig. 2 is an example of a flowchart for a practical and
27 robust electronic watermark detection method according to
28 the embodiment. First, at step 210 one frame (N samples)
29 is extracted from input digital data. At step 220, the

1 extracted frame is multiplied by a window function, and
2 at step 230 a Fourier transform is performed for the
3 resultant frame. As a result, the frequency component of
4 the frame is obtained. Then, at step 240, the frequency
5 components of the frame transformed in the frequency
6 domain are stored in a number equivalent to a
7 predetermined frame count. When the count of the stored
8 frequency components equals the predetermined frame
9 count, a search of the detected values is performed to
10 locate the greatest absolute value, which subsequently is
11 output as a frame shift (the head position of a unit).
12 This calculation is performed using a specific mask, and
13 a detected value is obtained with the assumption that the
14 specific frame is located at the head position. Finally,
15 at step 260, the detected value is selected, based on the
16 obtained frame shift, and is compared with the frequency
17 to determine the bit information for embedded additive
18 information.

19 Equations/Expressions

20 In the following description all equations relating to
21 the present invention are tabulated at the end of the
22 text portion of this specification just prior to the
23 claims. Each equation is given an expression number
24 which is indicated at the place in the text below where
25 the expression belongs.

26 Standard embedding and detection method

1 The processing performed by the embedding and detection
2 method of the embodiment will now be described.

3 Additive information to be embedded

4 First, additive information to be embedded is represented
5 as a symbol. The additive information consists of a bit
6 sequence of 1s and 0s, in which all the 0s are replaced
7 by -1s to prepare an array.

8 [Expression 1]

9 According to this method, each bit of the additive
10 information is allocated to a frequency band having a
11 specific width.

12 [Expression 2]

13 This expression indicates that the b-th bits from
14 frequency lower(b) to frequency upper(b) are allocated to
15 the frequency band, and that all the information C_w
16 embedded in the frequencies in this range is defined as
17 CB_b . The correlation between the bits and the frequency
18 band is the same for all the frames. Fig. 3 is a graph
19 showing that the frame axis (time axis) is perpendicular
20 to the frequency axis, and that the same bit is always
21 embedded in a specific frequency band (the same bit is
22 represented by the portions sharing the same pattern).

23 [Mask]

24 The mask is a matrix of +1s and -1s, and since the
25 embedding system and the detection system must both
26 understand the function of the same mask, for this
27 reason, the mask can serve as a type of secret key. For

1 the embedding system, the mask determines whether a
2 frequency component should be increased or decreased, and
3 for the detection system, the mask determines whether, in
4 the detection formula, a frequency component should be
5 added or subtracted.

6 [Expression 3]

7 [Extraction of samples]

8 N samples are extracted from digital audio data arranged
9 in a time series, in which the n-th sample of an
10 extracted frame f is represented by $a(f, n)$. Taken
11 collectively, these N samples form processing units
12 called frames, each of which overlaps half of a
13 succeeding frame. Fig. 4 is a diagram showing the
14 overlapping of frames.

15 [Windowing]

16 A window function is multiplied to perform a FFT for a
17 frame. Basically, a sine function is appropriate;
18 however, any other function that satisfies the following
19 expression can be employed. This guarantees that the
20 digital audio data will be recovered unless the
21 information is embedded when the frames are superimposed
22 after the windowing has been performed twice.

23 [Expression 4]

24 In this expression, n denotes a natural number that is
25 equal to or smaller than $N/2$. The sine window function
26 is

27 [Expression 5]

28 The windowing processing is

JP919990241US1

1 [Expression 6]

2 In this expression 6, n denotes a natural number equal to
3 or smaller than N .

4 [FFT]

5 An FFT is performed for $aw(f,n)$ to obtain frequency
6 component $F_{f,w}$.

7 [Power embedding]

8 During the embedding process, only the amplitude (power)
9 is changed, the phase is unchanged.

10 Fig. 5 is a graph for explaining the change in the
11 amplitude.

12 [Expression 7]

13 [IFFT]

14 An IFFT is performed for embedded frequency component
15 $F'_{f,w}$ to obtain $aw'(f,n)$.

16 [Windowing, superimposing frames and outputting them
17 along a time axis]

18 The frame is multiplied by the window function, then the
19 resultant frame is added to the succeeding frame and the
20 obtained frame is output. In this fashion, the embedding
21 of the frame in the digital audio data is completed.

22 [Expression 8]

23 According to this expression, the first half of a frame
24 is added to the preceding frame, and the second half of
25 the frame is added to the succeeding frame. Further, the
26 left side of the expression refers to the digital audio

1 data after the embedding has been completed. When this
 2 data has been output, the embedding process for the frame
 3 f is terminated. Fig. 6 is a diagram for explaining the
 4 windowing and superimposition of frames.

5 [Cycle synchronization]

6 The detection process is performed in the same manner as
 7 the embedding process, up until the FFT process is
 8 performed to obtain the frequency component. Thereafter,
 9 the amplitude $F_{f,w}$ is obtained for each frequency, and is
 10 stored in the buffer. When the storing of amplitudes has
 11 proceeded until the requirements for the frame F have
 12 been satisfied, cycle synchronization and bit detection
 13 can be initiated. Since one part of the digital audio
 14 data may be cut off, frame $f=1$ is not always the first
 15 frame when the information is embedded. If the frame is
 16 shifted, the mask and the amplitude to be multiplied
 17 differ, so that a correct bit can not be detected. Fig.
 18 7 is a diagram showing an example wherein no frame
 19 shifting has occurred, and Fig. 8 is a diagram showing an
 20 example wherein the shifting of one frame has occurred.
 21 Cycle synchronization is a process used to calculate S_s ,
 22 while assuming frame shift s , and to obtain s , with which
 23 the maximum S_s is provided. Fig. 9 is a diagram for
 24 explaining cycle synchronization. For s , all the
 25 integers from 0 to $(F-1)$ are attempted. The expression
 26 used to acquire S_s is the addition of the bit detection
 27 values. First, when frame shift s is assumed (i.e., C_w
 28 was -1 in the embedding process), the bit detection
 29 expression for bit 0 is represented by

1 [Expression 9]
2 And the bit detection expression for bit 1 (i.e., C_w was
3 +1 in the embedding process) is represented by
4 [Expression 10]
5 In this expression, masks for the first subscript ($f+s$)
6 in $M_{f+s,w}(c)$ are employed in mod F . The addition of these
7 masks to obtain the correct bit is the detection
8 expression used for cycle synchronization. However,
9 since it is unclear whether the b -th bit is +1 or -1,
10 greater values for the masks are selected and added
11 together.
12 [Expression 11]
13 The value s with which the maximum S_s is provided is the
14 answer for the frame shifting.

15 [Bit detection]
16 During bit detection, $C_{-,b(s)}$ and $C_{+,b(s)}$ are compared using
17 the frame shift s , obtained during the cycle
18 synchronization process, to determine a bit.
19 [Expression 12]

20 [Variation]
21 An explanation will now be given for an extension method
22 and a replacement method employed in order to improve the
23 basic performances of the embedding and detection
24 systems.

25 [Threshold watermark value and threshold bit value]
26 By using the frame shift s provided by cycle
27 synchronization, whether a watermark is embedded in the

1 digital audio data can be determined based on the
2 following expression.

3 [Expression 13]

4 TMW denotes a threshold constant set in advance. The
5 upper limit for in expression 13 may be reduced, so that
6 a detection value for a bit embedded in a frequency band
7 that is equal to or higher than a specific high frequency
8 can be ignored. Further, whether the detection results
9 obtained for each bit are reliable can also be
10 determined.

11 [Expression 14]

12 T_b denotes a threshold value for the b-th bit. A
13 constant difference for each bit can be employed as a
14 threshold value, so that a high threshold value can be
15 set for a bit that should be especially reliable.

16 [Employment of the same mask for several sequential
17 frames for information embedding]

18 When a mask is employed for embedding information for
19 several sequential frames, embedding signals in the
20 overlapped frames strengthen each other and improve the
21 detection efficiency. The same mask are employed for
22 embedding information for several sequential frames.

23 [Pairing of every two frequencies]

24 When the denominators of expressions 9 and 10 are smaller
25 than the numerators, the detection value can be

1 increased.

2 Of these methods, one involves the pairing of every two
3 frequencies and the employment of a difference as a
4 denominator. For the embedding, the sign of the odd
5 frequency of the mask must be set opposite the sign of
6 the succeeding arbitrary, even frequency. It should be
7 noted that w denotes an arbitrary natural number equal to
8 or smaller than $W/2$, and f denotes an arbitrary natural
9 number equal to or smaller than F . For detection, the
10 difference between two adjacent frequencies is obtained.
11 [Expression 15]

12 [Dividing a mask into two parts to increase the
13 calculation speed]

14 According to the above method, frame shifts of 0 to $(F-1)$
15 must be attempted during cycle synchronization, and
16 expressions 9 and 10 must be calculated for each F
17 attempts. Therefore, a mask is defined as the product of
18 two masks as follows.

19 [Expression 16]

20 When the mask is used for embedding, the detection
21 expression is represented by
22 [Expression 17]

23 This expression can be decomposed into
24 [Expression 18]

25 In this expression, $q_{b,f}$ does not depend on the frame
26 shift s , and it can be calculated before cycle
27 synchronization is initiated. Further, since $F_{f,q}$ need
28 not be stored in the buffer, the required storage

1 capacity is reduced.

2 [Changing the width of a frequency band, and
3 discriminating between the reliabilities of the
4 individual bits]

5 The additive information to be embedded can be
6 information concerning a copyright, copying and
7 reproduction permission information, or information
8 concerning music names and words, and the importance of
9 the additive information differs greatly, depending on
10 the information type. For example, generally the copying
11 and reproduction permission information is more important
12 than the music names, and is advantageously very robust.
13 According to the method of the invention, the
14 reliabilities of bits can be discriminated between by
15 changing the width of each frequency band. The width of
16 the frequency band is $\text{upper}(b) - \text{lower}(b) + 1$, and if the
17 width is increased, the robustness and the reliability of
18 the bit are increased. Fig. 10 is a graph showing an
19 example wherein a wide frequency band is allocated while
20 the half including additive information is regarded as
21 more important.

22 [Equalizing the reliabilities of bits]

23 Assume that the bits of additive information must have
24 equal reliability. When each bit in the degradation
25 process must have equal reliability, such as for a voice
26 compression technique or radio broadcasting, wherein a
27 band-pass filter is effective, the above method is not
28 adequate. Because when the low-pass filter is

1 functional, only the bit embedded in a high frequency
2 band is greatly deteriorated. Thus, all the bits are
3 embedded evenly in all the frequency bands. For example,
4 additive information to be embedded in frame f and
5 frequency w is obtained using the following expression,
6 and a bit is embedded diagonally.

7 [Expression 19]

8 The values in the parenthesis $\text{lower}(b-f-1)$ and
9 $\text{upper}(b-f-1)$ in this expression are mod B . The positions
10 represented by this expression for embedding individual
11 bits are as shown in Fig. 11. The rectangles having the
12 same pattern in Fig. 11 (representing positions in the
13 frequency/frame plane) are those carrying the same bit.
14 Since C_w is defined as $C_{f,w}$, the mask is defined as
15 $M_{f,w}(C_{f,w})$.

16 [Expression 20]

17 For embedding,

18 [Expression 21]

19 For detection,

20 [Expression 22]

21 The values in parenthesis, $\text{lower}(b+f-1)$ and $\text{upper}(b+f-1)$,
22 in this expression are mod B . In this embodiment, the
23 method for regularly embedding bits diagonally has been
24 explained; however, the embedding positions need not be
25 arranged diagonally. For example, a secret key can be
26 employed in the embedding process to determine a bit
27 embedding position, and it can be also employed in the

1 detection process to obtain the position of a frequency
 2 component used for bit detection. Then, a system that
 3 inhibits bit detection by a party who does not know the
 4 secret key can be mounted on the above described portion.

5 [Discrimination and equalization of reliability]

6 In addition, differences in reliability can be
 7 discriminated between while specific robustness relative
 8 to the bandpass filter is provided for each bit. As one
 9 method, as is shown in Fig. 12, lower(b) and upper(b) are
 10 changed for each frame. This means the extension to
 11 lower(f,b) and upper(f,b). So long as the embedding and
 12 detection systems understand the differences between the
 13 lower(f,b) and upper(f,b), an arbitrary value can be
 14 employed. In Fig. 12, the same bit is embedded
 15 diagonally; however, the diagonal arrangement is not
 16 necessarily required. The array of the additive
 17 information is defined as

18 [Expression 23]

19 Further, the bit detection expression is defined as
 20 [Expression 24]

21 [Discrimination and equalization of reliability and an
 22 increase in processing speed]

23 The method for increasing the processing speed will now
 24 be described. The following restrictions are provided
 25 for upper(f,b) and lower(f,b).

26 * The upper(f,b)-lower(f,b)+1 width of the frequency band
 27 is limited to several types.

1 * For bit embedding positions, only bits having the same
 2 width as the frequency band can be replaced.
 3 Fig. 13 is a diagram for explaining diagonal bit
 4 embedding that can increase the processing speed. For
 5 example, in Fig. 13 the frequency bands are limited to
 6 two types, and less reliable bits are embedded diagonally
 7 in several narrow frequency bands, while reliable bits
 8 are embedded diagonally in wide frequency bands.

9 [Case wherein additive information is embedded using the
 10 positive and negative values of a mask]

11 According to the above method, different masks are
 12 employed for embedding bit 1 and for embedding bit 0.
 13 However, bits can be discriminated between and embedded
 14 by using the positive and negative values of one mask.
 15 In this case, only one mask is required.

16 [Expression 25]

17 For embedding, an increase or a reduction is determined
 18 in accordance with a bit.

19 [Expression 26]

20 For both cycle synchronization and bit determination,
 21 only one detection expression is formed, as follows.

22 [Expression 27]

23 As a result of this expression, both positive and
 24 negative values are obtained. In this case, it is
 25 assumed that the first subscript in mask $M_{f+s,w}$ is used for
 26 mod F. For cycle synchronization, the absolute values
 27 are obtained and added together so as to acquire the
 28 maximum, total value.

JP919990241US1

1 [Expression 28]

2 Bit determination is performed by using the positive and
3 negative detection values.

4 [Expression 29]

5 [Returning an embedding signal to a time domain, and
6 embedding]

7 When the embedding processing is changed as follows, an
8 error that accompanies windowing or a FFT can be reduced.

9 (1) Extraction of samples

10 (2) Windowing

11 (3) FFT

12 (4) Generation of an embedding signal

13 The auditory psychological model is applied for a
14 frequency component to calculate a permissible range
15 wherein a human being can not discern a difference, even
16 when the frequency component is changed. An embedding
17 signal is prepared within the permissible range.

18 (5) IFFT

19 An IFFT is performed for the embedding signal.

20 (6) Windowing and superimposing frames, and returning the
21 results along a time axis

22 The resultant frame is multiplied by a window function,
23 and this frame is superimposed on an adjacent frame, so
24 that the embedding signal can be obtained in the time
25 domain.

26 (7) Addition of the frame to digital audio data

27 When the obtained frame is added to the original digital
28 audio data, the digital audio data carrying the embedding
29 signal is acquired and output.

1 For (4), the embedding signal is prepared using the
2 following expression.
3 [Expression 30]

4 [Employment of the same mask]
5 When the masks that correspond to all the frequencies
6 included in one frequency band are equalized, robustness
7 relative to the frequency shift can be provided for the
8 audio data. For example, when 5000Hz is changed to
9 5050Hz due to a frequency shift, and when different masks
10 (signs) are used for 5000Hz and 5050Hz, the detection is
11 adversely affected. However, when the same mask (sign)
12 is employed, there is no adverse effect.

13 [Change in the width of a frequency band in accordance
14 with a frequency]
15 Finally, when the width of a frequency band is extended
16 as a frequency increases, robustness relative to an
17 overall change in the frequency, due to a change in the
18 music reproduction speed and a change in the length of a
19 frame, can be provided. For this reason, since all the
20 frequencies are increased by 10% when the reproduction
21 speed is increased by 10%, 500Hz is changed to 550Hz and
22 5000Hz is changed to 5500Hz. Therefore, for a higher
23 frequency the frequency shift is greater, and in order to
24 provide for all the frequencies the robustness relative
25 to a frequency shift, for a higher frequency a wider
26 frequency band is necessary.

1 [Reducing a frame length to be detected]
2 When the length of a window (i.e., the length of a frame)
3 for detection is shorter than the length of a window for
4 embedding, the effect on the end of the frame being
5 embedded can be reduced. For example, when a mask having
6 the same sign is employed in the frequency band, assume
7 that for embedding one frame consists of N samples and
8 that for detection one frame consists of N/2 samples. As
9 a result, the effect produced by the sign that was
10 embedded in the k-th frequency is observed in the k/2-th
11 frequency. And when one frame consists of N/4 samples
12 for detection, the effect produced by the embedding in
13 the k-th frequency is observed in the k/4-th frequency.
14 This is because, according to the property of a Fourier
15 transform, when the frame length for observation is
16 reduced by half, the frequency resolution that is
17 observed is also reduced by half. That is, in the
18 detection process, when the sign of a mask is shifted a
19 distance equivalent to the difference of a frame length,
20 detection is enabled even when the frames differ. In
21 this embodiment, overlapping of half or less of frames
22 occurs, and signs are embedded while also being changed
23 along a time axis. However, when in a specific frequency
24 band, between adjacent frames along the time axis the
25 signs of masks differ, the embedding effect is canceled
26 out at the portion whereat the frames overlap (for
27 example, when the signs are "++--" and the overlapping
28 portions of the second and third frames differ). When a
29 short frame length is employed for detection, as is
30 described above, detection is enabled only for a portion

1 that is less affected by an adjacent frame.

2 <Second Embodiment>

3 An explanation will now be given for a second example
 4 embodiment of the present invention, which provides a
 5 practical and robust electronic watermark for digital
 6 audio data and which will prevent the unauthorized
 7 analyzation of an embedded additive information
 8 algorithm. In the following description, "sample" is the
 9 expression used when audio data is the target; however,
 10 the present invention can be applied for a moving picture
 11 by replacing "sample" with "frame", and for a static
 12 picture by replacing "sample" with "pixel".

13 [Determining a random embedding start position]

14 Before embedding, the first R samples of the content are
 15 skipped, and the embedding is performed beginning at the
 16 (R+1)-th sample. Here, R denotes a random variable
 17 determined before embedding is initiated.

18 [Determining a random embedding start bit or frame]

19 To embed multiple bits, a start bit can be determined at
 20 random. This is applicable only in a case wherein before
 21 detection a detector performs a process for determining
 22 the first bit. In this case, since the first bit should
 23 be found through this process, that bit need not always
 24 be embedded in the head of the content. The following
 25 method can be employed as a modification. According to a
 26 method for defining a specific number (F) of samples as
 27 one unit and for embedding one or multiple bits therein,

1 the process for finding the location whereat the
2 pertinent unit begins is performed during the detection
3 process. Once the head is found, the head of the content
4 need not match the head of the unit. Thus, the sample of
5 the unit used for the embedding start can be determined
6 at random. Fig. 17 is a diagram showing an embedding
7 start unit, and Fig. 18 is a diagram showing a virtual
8 embedding start point.

9 [Adding random noise]

10 Not only an embedding signal, but also noise calculated
11 at random is added to the content. If the amount of
12 noise added is sufficiently small, tone quality can be
13 prevented from being affected. And if only random noise
14 added, it can be expected that the detection results will
15 also be less affected.

16 [Occasionally adding merely a random signal, without
17 performing embedding]

18 During the embedding process, a portion whereat only a
19 random signal is to be added without performing embedding
20 is prepared at a timing determined at random. Although
21 this method slightly affects the detection results, since
22 bits in other portions of the content can be detected,
23 this method can be employed when no problem occurs, even
24 when there are portions in which no bits are embedded.

25 [Performing a pre-process before embedding]

26 Before the embedding process, a random pre-process is
27 performed to handle the content.

28 Fig. 14 is a diagram for explaining a pre-process and a

1 post-process for the embedding process.

2 Content 0 before being processed [pre-process] content 0'
3 after the pre-process and before the embedding, and
4 [embedding] content 0'' after embedding.

5 When this process is performed internally, a larcenous
6 user can have no knowledge of the "content 0' after the
7 pre-process and before the embedding". Therefore, even
8 if the larcenous user knows the difference between the
9 "content 0 before being processed" and the "content 0''
10 after the embedding", $D = 0'' - 0$, he or she will have no
11 knowledge of the difference between the "content 0''
12 after the embedding" and the "content 0' after the
13 pre-process and before the embedding", $D' = 0'' - 0'$. The
14 difference D' includes both the effect D , obtained by
15 embedding, and the effect $D' = 0' - 0$, provided by the
16 pre-process, and this prevents the embedding algorithm
17 from being identified. An example pre-process is the
18 overlapping, insertion or omission of a sample, the
19 shifting of a sample, or the expansion/compression of a
20 sample.

21 [Overlapping, insertion or omission of a sample]
22 For content, a sample is omitted, a specific sample is
23 repeated, or a specific sample is inserted. This
24 process, for music, is generally called "pitch-preserved
25 time expansion/compression". So long as the omission,
26 overlapping or insertion frequency is sufficiently low
27 (e.g., one sample every 44100 samples per second), the

109894043-062804

1 tone quality is not at all affected. For a static
2 picture, this process corresponds to the overlapping,
3 insertion or omission of a horizontal line or a vertical
4 line. For a moving picture, a horizontal line or a
5 vertical line for each static picture may be overlapped,
6 inserted or omitted, or a static picture (a frame) may as
7 one unit be overlapped, inserted or omitted. If the
8 affect on the tone quality or the image quality is kept
9 especially small, the location for the overlapping,
10 insertion or omission of the image must be selected in
11 accordance with the characteristic of the content (this
12 is also generally performed in the pitch-preserved time
13 expansion/compression process). For example, the target
14 location for the omission, overlapping or insertion is
15 limited to the portion wherein similar samples are
16 continued. If the number of samples reduced by omission
17 is adjusted so it is the same as the number of samples
18 increased by overlapping or insertion, the length of the
19 resultant content after the process can be the same as
20 the length of the content before the process.

21 [Shifting of a sample]

22 The content is shifted a distance equivalent to the
23 number of random samples. In other words, a sample is
24 added to the head of the content, or is removed from the
25 head. The number of samples is not always an integer.
26 When the random sample count is a real number other than
27 an integer, the sample values of the content are
28 determined by interpolation. For example, when linear
29 interpolation is employed, the sample value is changed by

1 using
2 [Expression 31]
3 In this expression, $[r]$ denotes a maximum integer that
4 does not exceed r , $v(x)$ denotes an x -th sample value
5 before the process, and $v'(x)$ denotes an x -th sample
6 value after the process.

7 [Expansion/compression]
8 A slight expansion/compression of the content can be
9 performed for the object of this embodiment. For
10 example, when the content is linearly expanded or
11 compressed an amount that is equal to or smaller than 1%,
12 the change can not be discerned by human beings.
13 Further, a portion of the content may be expanded and
14 another portion may be compressed, so that the length of
15 the content is maintained. These methods provide great
16 effects, even when the random pre-process is not
17 employed. In other words, even if the pre-process is a
18 decisive algorithm, obtaining the difference D'' is
19 difficult, so long as the algorithm can not be
20 identified.

21 [Performing the post-process after the embedding]
22 When the same process used for the above method, while
23 performing the pre-process for the embedding, is used to
24 perform the post-process for the content produced by the
25 embedding, the same effects that prevent the analyzation
26 of an embedding signal can be provided. In this case,
27 since the embedding signal has also been processed, the
28 robustness relative to the analyzation may be increased.

1 However, since the embedding signal is slightly
2 deteriorated when this post-process is performed, it is
3 predicted that the detection capability will be slightly
4 reduced.

5 [Calculation of an embedding signal after re-sampling]
6 This method is similar to the method used to perform the
7 pre-process before the embedding, except that the
8 original content is not changed. For a moving picture
9 and a static picture, the re-sampling corresponds to a
10 change in the number of pixels. The processing used for
11 this method is performed as follows. Fig. 15 is a
12 diagram for explaining the method for performing
13 re-sampling and then calculating an embedding signal.

14 * A sampling frequency of the content 0 before the
15 processing is defined as r .
16 * The content 0 is re-sampled, at a sampling frequency
17 r' , to obtain the content 0' after the re-sampling.
18 * A temporary embedding signal E' is obtained for the
19 content 0'. The sampling frequency for the signal E' is
20 also r' .
21 * The temporary embedding signal E' is re-sampled, at the
22 sampling frequency r , to obtain an embedding signal E .
23 * The embedding signal E is added to the content 0 to
24 obtain the content 0'' after the embedding.

25 As another method, as is shown in Fig. 16 (performing re-
26 sampling and then calculating an embedding signal),
27 * A sampling frequency of the content 0 before the

1 processing is defined as r .
 2 * The content 0 is re-sampled, at a sampling frequency
 3 r' , to obtain the content 0' after the re-sampling.
 4 * A temporary embedding signal E' is obtained for the
 5 content 0'. The sampling frequency for the signal E' is
 6 also r' .
 7 * The temporary embedding signal E' is added to the
 8 content 0', to prepare the content 0'', after the
 9 embedding is performed at the sampling frequency r' .
 10 * The content 0'' is re-sampled, at the sampling
 11 frequency r to obtain the content 0'''.

12 The sampling frequency used for embedding may be
 13 determined at random for the embedding process. Even
 14 when the sampling frequency is not determined at random,
 15 it is considered to be an effective means for hiding the
 16 algorithm. According to this method, when the sample
 17 count (the unit in Figs. 17 and 18) is employed as a
 18 reference to generate an embedding signal, identifying
 19 the length of the samples is difficult.

20 [Setting a random interval for outputting detection
 21 results]
 22 This is not a method for substantially preventing the
 23 analyzation of a difference; however, since this method
 24 is the same as another method used to for prevent the
 25 analyzation of an algorithm, this method will be
 26 explained. According to this method, when the detection
 27 results are obtained, instead of an action such as the
 28 display of results or the halting of copying, the output

1 is intentionally delayed at specific, randomly determined
2 time intervals. Therefore, the minimum time required for
3 detection is prevented from being identified by a
4 larcenous user.

5 [Time change of bit information embedding position]
6 When N bits ($N \geq 1$) of information is to be embedded as an
7 electronic watermark in image or audio content, the
8 embedding position for each bit of the bit information
9 embedding unit (hereafter referred to as a unit) is
10 changed as time elapses. Thus, even when a specific
11 position in the bit information embedding content is
12 processed or destroyed, disabling of the detection or the
13 alteration of only specific bit information can be
14 avoided. Further, even when the information is the same,
15 it is embedded in different positions, so that the
16 embedding signals do not strengthen each other even if
17 the average of multiple contents is obtained. This is
18 advantageous as it makes it difficult to analyze the
19 electronic watermarking algorithm and the key. Assuming
20 that the n -th bit information embedding position at time
21 t (unit number) is defined as $P(n,t)$, the n -th bit
22 information embedding position at time $t+1$ can be
23 represented by $P(n,t+1)=F(P(n,t))$. $F(P)$ denotes a
24 transform operator for changing a bit information
25 embedding position, and P and $F(P)$ have a specific cycle
26 T .

27 [Expression 32]

28 Fig. 19 is a diagram showing an example of P and $F(P)$

1 wherein four bits of information is embedded in one unit.
 2 Each block indicated by a solid line in Fig. 19
 3 represents a unit, and the small numbered blocks in the
 4 units represent the positions used for embedding bit
 5 information.

6 In this example,
 7 $P(n,t) = t+n \text{ mode } 4$ ($T=4$, $n=0, 1, 2, 3$).
 8 When $F(P)$ is complicated and the length is extended, it
 9 is more difficult to assume the bit information embedding
 10 position and to disable the detection of specific bit
 11 information and to alter specific bit information.

12 Further, as time elapses, not only the bit information
 13 embedding position, but also the interpretation of the
 14 embedded information can be changed. In addition,
 15 according to this method, when the original target
 16 content for electronic watermarking has a correlation
 17 along the time axis, the correlation can be canceled
 18 because the bit information embedding position is changed
 19 as time elapses. As a result, a false positive error
 20 ratio, at which the presence of embedded information is
 21 determined, even though no information is actually
 22 present, can be reduced.

23 [Detection]

24 Since the bit information embedding position in the unit
 25 is changed as time elapses, the embedded information
 26 should be detected in the following manner for each cycle
 27 of the change in the bit information embedding position.

1 [Expression 33]

2 In this expression, $D(P(n,t))$ denotes an operator for
3 electronic watermark detection at the information
4 embedding position in each unit, and D_n denotes a
5 detection value. When the information embedding bit
6 count $N \geq 2$, and when the content in which information is
7 embedded is processed, the position of a detection value
8 that represents the first information embedding bit can
9 not be identified. Thus, the position of the first
10 information embedding bit must be detected. This method
11 will now be described.

12 When the information embedding bit count $N \geq 2$, the
13 detection value D_n that represents the position of the
14 first information embedding bit is detected using one of
15 the following methods.

16 [Insertion of position where no information is to be
17 embedded]

18 At the same cycle T as the bit information embedding
19 position change cycle T , a position whereat no
20 information is to be embedded is inserted as a mark for
21 detecting the first embedded bit. For example, in P and
22 $F(P)$ in Fig. 19, a portion shown in Fig. 20, whereat no
23 information is to be embedded, is inserted. Assume that
24 the shaded portions in Fig. 20 are those whereat no
25 information is to be embedded in the frame. When the
26 detection value of the information embedding position
27 satisfies $|D_n| > Th$, the n -th detection value that

1 satisfies $\min(|D_n|) < T_h$ can be obtained as a mark for
2 locating the first embedded bit. It should be noted that
3 T_h is a specific threshold value.

4 [Embedding of information for which the bit is inverted
5 at cycle $2T$]

6 At the same cycle T as the bit information embedding
7 position change cycle T , information for which the bit is
8 inverted at cycle $2T$ is embedded. Fig. 21 is a diagram
9 showing an example of the embedding of information for
10 which the bit is inverted at cycle $2T$. Assume that + or
11 - in Fig. 21 represents the bit-inversion information.
12 During the detection process, at cycle $2T$ each detection
13 value is calculated based on expression 33, and the n -th
14 detection value that satisfies expression 34 is examined.
15 [Expression 34]

16 Then, the first bit of the embedded information can be
17 obtained. In this case, the following expression is
18 established.

19 [Expression 35]

20 [Use of information other than bit information]

21 The detection value of another signal is employed to
22 detect the first bit for embedded information. For
23 example, when unit positioning information (sink
24 information) is embedded for the electronic watermark
25 detection, during the bit information embedding process
26 the sign of the pertinent signal is inverted for each
27 embedding position change cycle T . Or, a portion having
28 an inverted sign is inserted each cycle T . As a result,

1 in the detection process, when the portion is examined
2 whereat the sign of the positioning information is
3 changed, the position of the first bit can be obtained.
4 Fig. 22 is a diagram showing an example for using
5 information other than the bit information.

6 [Change of interpretation of embedded information]
7 To repetitively embed a specific bit in content, the sign
8 of the bit is inverted in accordance with a specific sign
9 sequence. Since the same information is not constantly
10 embedded, the analyzation of information is difficult.
11 The information to be embedded at a specific time is
12 calculated using the following expression.
13 [Expression 36]

14 In this expression, B denotes the original bit
15 information (1 or -1; a bit is represented as 0 or -1),
16 and B'(t) denotes a bit, which is actually embedded in
17 the content, having a sign that is inverted as time
18 elapses. M(t) denotes a sign sequence for inverting the
19 embedded information, and a value +1 or -1 is provided.
20 As is described above, when the interpretation of the
21 embedded information is to be changed as time elapses,
22 the detection values Dn should also be obtained by using
23 the interpretation change method M(t) as in
24 [Expression 37]

25 However, it should be noted that when the content in
26 which the information is being embedded is processed, the
27 detection of the value $D(P(n, T))$ at each position P(n,
28 t) must be synchronized with M(t). When the correct

1 synchronization is acquired, $M(t)$ is multiplied twice
 2 during the embedding and the detection processes to
 3 provide a value of +1, so that the original bit
 4 information can be obtained. To synchronize the process,
 5 one of the following methods is employed.

6 [+/- inversion]

7 Assume $M(t+1) = -M(t)$ is the interpretation method $M(t)$.
 8 In order to correctly interpret the embedded bit
 9 information, first, the value $D(P(n,t))$ detected at each
 10 location $P(n,t)$ is multiplied by a sequence wherein signs
 11 are inverted at adjacent times, and the detection value
 12 D_n is obtained. When correct synchronization with $M(t)$
 13 is acquired, the bit information can be correctly
 14 detected. When the correct synchronization is not
 15 obtained, all the signs + and - are inverted, and the
 16 resultant sign sequence is multiplied by each value
 17 $D(P(n,t))$. Thus, the inverted bit information is
 18 detected. Therefore, information W_m for determining
 19 whether the inverted bits are detected is embedded at a
 20 position other than the bit information embedding
 21 position. When the embedded bit information is detected,
 22 the sign of the information W_m is examined, and the bit
 23 information is re-interpreted as [Expression 38]
 24 Then, the embedded bit information is obtained.

25 [Application of the maximum detection value]

26 A sequence is prepared that has, as the interpretation
 27 change method $M(t)$, a cycle T' , and has the maximum value
 28 T' only when

1 [Expression 39]
2 is established with $j = m \cdot T$ (m is a natural number).
3 During the detection process, the detection values are
4 calculated by shifting the method $M(t)$, and the shifting
5 distance required to provide the maximum detection value
6 is obtained to effect the synchronization with the
7 interpretation change method $M(t)$.
8 [Expression 40]

9 [Employment of information other than bit information]
10 The detected bit interpretation $M(t)$ is provided as the
11 detection value for another signal. For example, when
12 unit positioning information (sink information,
13 represented as $S(t)$) is embedded for electronic watermark
14 detection, during the embedding of the bit information,
15 the sign to which the pertinent signal is inverted is the
16 same as that sign of the $M(t)$. During the detection
17 process, the sink information is detected, and its sign
18 for the sink information is used for bit interpretation.
19 [Expression 41]

20 According to the present invention, a practical and
21 robust electronic watermarking method and system are
22 provided that do not require the embedding of a frame
23 synchronization signal. Further, since frame
24 synchronization is not required, the detection time can
25 be reduced. In addition, the storage capacity normally
26 required for a detection system to provide frame
27 synchronization is not necessary. Thus, an electronic
28 watermarking method and system are provided that make it

1 difficult for a larcenous third party to analyze an
2 embedding algorithm.

3 The present invention can be realized in hardware,
4 software, or a combination of hardware and software. The
5 present invention can be realized in a centralized
6 fashion in one computer system, or in a distributed
7 fashion where different elements are spread across
8 several interconnected computer systems. Any kind of
9 computer system - or other apparatus adapted for carrying
10 out the methods described herein - is suitable. A typical
11 combination of hardware and software could be a general
12 purpose computer system with a computer program that,
13 when being loaded and executed, controls the computer
14 system such that it carries out the methods described
15 herein. The present invention can also be embedded in a
16 computer program product, which comprises all the
17 features enabling the implementation of the methods
18 described herein, and which - when loaded in a computer
19 system - is able to carry out these methods.

20 Computer program means or computer program in the present
21 context mean any expression, in any language, code or
22 notation, of a set of instructions intended to cause a
23 system having an information processing capability to
24 perform a particular function either directly or after
25 conversion to another language, code or notation and/or
26 reproduction in a different material form.

1 It is noted that the foregoing has outlined some of the
 2 more pertinent objects and embodiments of the present
 3 invention. This invention may be used for many
 4 applications. Thus, although the description is made for
 5 particular arrangements and methods, the intent and
 6 concept of the invention is suitable and applicable to
 7 other arrangements and applications. For example, in
 8 many applications and/or embodiments of the present
 9 invention the term 'including' as used herein in this
 10 description and in some of the claims often is also given
 11 the meaning of the words 'consisting of'. It will be
 12 clear to those skilled in the art that other
 13 modifications to the disclosed embodiments can be
 14 effected without departing from the spirit and scope of
 15 the invention. The described embodiments ought to be
 16 construed to be merely illustrative of some of the more
 17 prominent features and applications of the invention.
 18 Other beneficial results can be realized by applying the
 19 disclosed invention in a different manner or modifying
 20 the invention in ways known to those familiar with the
 21 art.

22 The following is a tabulation of the equations relating
 23 to the present invention. The expression number of each
 24 equation corresponds with the expression number given at
 25 the place in the text above where the expression belongs.

[Expression 1]

$$\begin{aligned} CB &= [CB_1, CB_2, \dots, CB_b, \dots, CB_B] \\ &= [+1, +1, \dots, -1, \dots, +1] \end{aligned}$$

[Expression 2]

$$C_w = CB_b \quad (\text{lower}(b) \leq w \leq \text{upper}(b))$$

[Expression 3]

$$M = \begin{bmatrix} M_{1,1}(C_1) & \dots & M_{1,W}(C_W) \\ \vdots & M_{f,w}(C_w) & \vdots \\ M_{F,1}(C_F) & \dots & M_{F,W}(C_W) \end{bmatrix}$$

[Expression 4]

$$w(n)^2 + w(n+N/2)^2 = 1$$

[Expression 5]

$$w(n) = \sin\left(\pi \frac{n}{N}\right)$$

[Expression 6]

$$aw(f,n) = w(n) \times a(f,n)$$

[Expression 7]

$$F'_{f,w} = F_{f,w} \times \left\{ 1 + M_{f,w}(C_w) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

$$I'_{f,w} = I_{f,w} \times \left\{ 1 + M_{f,w}(C_w) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

$$R'_{f,w} = R_{f,w} \times \left\{ 1 + M_{f,w}(C_w) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

[Expression 8]

$$a'(f,n) = \begin{cases} w(n) \times aw'(f,n) + w(n+N/2) \times aw'(f-1,n+N/2) & (0 < n \leq N/2) \\ w(n) \times aw'(f,n) + w(n-N/2) \times aw'(f+1,n-N/2) & (N/2 < n \leq N) \end{cases}$$

[Expression 9]

$$c_{-,b}(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^F \left[\frac{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} M_{f+s,w}(-1) \times F_{f,w}}{\sqrt{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} (F_{f,w})^2}} \right]$$

[Expression 10]

$$c_{+,b}(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^F \left[\frac{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} M_{f+s,w}(+1) \times F_{f,w}}{\sqrt{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} (F_{f,w})^2}} \right]$$

[Expression 11]

$$S_s = \sum_{b=1}^B \max\{c_{-,b}(s), c_{+,b}(s)\}$$

[Expression 12]

$$b\text{-th bit} = \begin{cases} 1 & (c_{+,b}(s) > c_{-,b}(s)) \\ 0 & (c_{+,b}(s) < c_{-,b}(s)) \end{cases}$$

[Expression 13]

$$\text{Watermark} = \begin{cases} \text{Yes} & \left(\frac{1}{\sqrt{B}} \sum_{b=1}^B \max\{c_{-,b}(s), c_{+,b}(s)\} > TWM \right) \\ \text{No} & \text{otherwise} \end{cases}$$

[Expression 14]

$$b\text{-th bit} = \begin{cases} 1 & (c_{+,b}(s) - c_{-,b}(s) > T_b) \\ 0 & (c_{-,b}(s) - c_{+,b}(s) > T_b) \\ \text{No reliable bit information} & \text{otherwise} \end{cases}$$

[Expression 15]

$$c_b = \frac{1}{\sqrt{F}} \sum_{f=1}^F \left[\frac{\sum_{w=\frac{\text{lower}(b)}{2}}^{\frac{\text{upper}(b)}{2}} M_{f,2w-1} (F_{f,2w-1} - F_{f,2w})}{\sqrt{\sum_{w=\frac{\text{lower}(b)}{2}}^{\frac{\text{upper}(b)}{2}} (F_{f,2w-1} - F_{f,2w})^2}} \right]$$

[Expression 16]

$$M_{f,w} = MF_f \times MW_w$$

[Expression 17]

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^F \left[\frac{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} M_{f+s,w} F_{f,w}}{\sqrt{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} (F_{f,w})^2}} \right]$$

$$= \frac{1}{\sqrt{F}} \sum_{f=1}^F \left[MF_{f+s} \frac{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} MW_w F_{f,w}}{\sqrt{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} (F_{f,w})^2}} \right]$$

[Expression 18]

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^F [MF_{f+s} \times q_{b,f}]$$

$$q_{b,f} = \frac{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} MW_w F_{f,w}}{\sqrt{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} (F_{f,w})^2}}$$

[Expression 19]

$$C_{f,w} = CB_b \quad (\text{lower}(b-f+1) \leq w \leq (\text{upper}(b-f+1)))$$

[Expression 20]

$$M = \begin{bmatrix} M_{1,1}(C_{1,1}) & \dots & M_{1,w}(C_{1,w}) \\ \vdots & M_{f,w}(C_{f,w}) & \vdots \\ M_{F,1}(C_{F,1}) & \dots & M_{F,w}(C_{F,w}) \end{bmatrix}$$

[Expression 21]

$$F'_{f,w} = F_{f,w} \times \left\{ 1 + M_{f,w}(C_{f,w}) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

[Expression 22]

$$c_{+,b} = \frac{1}{\sqrt{F}} \sum_{f=1}^F \left[\frac{\sum_{w=\text{lower}(b-f+1)}^{\text{upper}(b-f+1)} M_{f,w}(+1) \times F_{f,w}}{\sqrt{\sum_{w=\text{lower}(b-f+1)}^{\text{upper}(b-f+1)} (F_{f,w})^2}} \right]$$

$$c_{-,b} = \frac{1}{\sqrt{F}} \sum_{f=1}^F \left[\frac{\sum_{w=\text{lower}(b-f+1)}^{\text{upper}(b-f+1)} M_{f,w}(-1) \times F_{f,w}}{\sqrt{\sum_{w=\text{lower}(b-f+1)}^{\text{upper}(b-f+1)} (F_{f,w})^2}} \right]$$

[Expression 23]

$$C_{f,w} = CB_b \quad (\text{lower}(f,b) \leq w \leq (\text{upper}(f,b)))$$

[Expression 24]

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^F \left[\frac{\sum_{w=\text{lower}(f,b)}^{\text{upper}(f,b)} M_{f+s,w} \times F_{f,w}}{\sqrt{\sum_{w=\text{lower}(f,b)}^{\text{upper}(f,b)} (F_{f,w})^2}} \right]$$

[Expression 25]

$$M = \begin{bmatrix} M_{1,1} & \dots & M_{1,W} \\ \vdots & M_{f,w} & \vdots \\ M_{F,1} & \dots & M_{F,W} \end{bmatrix}$$

[Expression 26]

$$\begin{aligned} F'_{f,w} &= F_{f,w} \times \left(1 + M_{f,w} \times \frac{P_{f,w}}{F_{f,w}} \right) \\ I'_{f,w} &= I_{f,w} \times \left(1 + M_{f,w} \times \frac{P_{f,w}}{F_{f,w}} \right) \\ R'_{f,w} &= R_{f,w} \times \left(1 + M_{f,w} \times \frac{P_{f,w}}{F_{f,w}} \right) \end{aligned}$$

TOP SECRET E4046860

[Expression 27]

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^F \left[\frac{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} M_{f+s,w} F_{f,w}}{\sqrt{\sum_{w=\text{lower}(b)}^{\text{upper}(b)} (F_{f,w})^2}} \right]$$

[Expression 28]

$$S_s = \sum_{b=1}^B |C_b(s)|$$

[Expression 29]

$$\text{b-th bit} = \begin{cases} 1 & (c_b(s) > 0) \\ 0 & (c_b(s) < 0) \end{cases}$$

[Expression 30]

$$\Delta F_{f,w} = M_{f,w}(C_w) \times P_{f,w} \times \frac{F_{f,w}}{F_{f,w}}$$

$$\Delta I_{f,w} = M_{f,w}(C_w) \times P_{f,w} \times \frac{I_{f,w}}{F_{f,w}}$$

$$\Delta R_{f,w} = M_{f,w}(C_w) \times P_{f,w} \times \frac{R_{f,w}}{F_{f,w}}$$

[Expression 31]

$$v'(x) = ([x+r] + 1 - (x+r)) \times v([x+r]) + ((x+r) - [x+r]) \times v([x+r] + 1)$$

[Expression 32]

$$P(n, t + T) = F^T(P(n, t)) = P(n, t)$$

[Expression 33]

$$D_n = \sum_{i=0}^{T-1} D(F^i(P(n, t + i)))$$

[Expression 34]

$$D0_n \cdot D1_n < 0$$

[Expression 35]

$$D0_n = \sum_{i=0}^{T-1} D(F^i(P(n, t + i)))$$

$$D1_n = \sum_{i=T}^{2T-1} D(F^i(P(n, t + i)))$$

[Expression 36]

$$B'(t) = B \times M(t)$$

[Expression 37]

$$D_n = \sum_{i=0}^{T-1} D(F^i(P(n, t + i))) \times M(t)$$

[Expression 38]

$$\begin{aligned} D_n &= D_n \text{ (if } Wm_{bitrev} > 0) \\ D_n &= -D_n \text{ (if } Wm_{bitrev} < 0) \end{aligned}$$

[Expression 39]

$$Conv(j) = \sum_{i=0}^{T-1} M(t+j+i) \times M(t+i)$$

[Expression 40]

$$D_n = \max_{0 \leq j \leq T'} \left(\sum_{i=0}^{T-1} D(F^i(P(n, t+i))) \times M(t+j) \right)$$

[Expression 41]

$$D_n = \sum_{i=0}^{T-1} D(F^i(P(n, t+i))) \times \sin(S(t))$$